

---

**Varnost strojev – Deli krmilnih sistemov v zvezi z varnostjo – 1. del:  
Splošna načela načrtovanja (enakovreden ISO 954-1:1996)**

Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze

Deskriptorji: varnost strojev, krmilne naprave, načrtovanje, vmesniki, nevarnosti, načela, napake, verifikacija

---

ICS 13.110

Referenčna številka  
SIST EN 954 –1:2000 (sl)

Nadaljevanje na straneh II in III in od 2 do 33

## NACIONALNI UVOD

Standard SIST EN 954-1 (sl), Varnost strojev – Deli krmilnih sistemov, v zvezi z varnostjo – 1. del: Splošna načela načrtovanja, prva izdaja, 2003, ima status slovenskega standarda in je enakovreden evropskemu standardu EN 954-1 (en), Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 1996.

## NACIONALNI PREDGOVOR

Evropski standard EN 954-1:1998 je pripravil tehnični odbor Evropskega komiteja za standardizacijo CEN/TC 114, Varnost strojev in naprav, katerega sekretariat sodi pod Osrednje tajništvo CEN. Pripravo tega standarda sta CEN poverila Evropska komisija in Evropsko združenje za prosto trgovino. Ta evropski standard ustreza bistvenim zahtevam evropske direktive 98/37/ES.

Slovenski tehnični odbor SIST/TC VSN Varnost strojev in naprav je dne 2000-06-00 privzel evropski standard EN 954-1:1998 po metodi ponatisa. Standard v slovenskem jeziku je le jezikovna različica.

## ZVEZA S STANDARDI

S prevzemom tega evropskega standarda veljajo za omejeni namen referenčnih standardov vsi standardi, navedeni v izvorniku, razen tistih, ki so že sprejeti v nacionalno standardizacijo:

SIST EN 292-1:1996	Varnost strojev - Osnovni pojmi, splošna načela načrtovanja - 1. del: Osnovna terminologija, metodologija
SIST EN 292-2:1996	Varnost strojev - Osnovni pojmi, splošna načela načrtovanja - 2. del: Tehnična načela in specifikacije
SIST EN 292-2:1996/A1:2000	Varnost strojev - Osnovni pojmi, splošna načela načrtovanja - 2. del: Tehnična načela in specifikacije - Dopolnilo A1
SIST EN 418:1999	Varnost strojev - Oprema za izklop v sili - Funkcionalni vidiki, načela načrtovanja
SIST EN 457:1998	Varnost strojev - Slišni nevarnostni signali - Splošne zahteve, načrtovanje in preskušanje (ISO 7731:1986, modificiran)
SIST EN 614-1:1998	Varnost strojev – Načela ergonomskega načrtovanja – 1. del: Terminologija in splošna načela
SIST EN 842:1998	Varnost strojev - Vidni nevarnostni signali - Splošne zahteve, načrtovanje in preskušanje
SIST EN 981:1998	Varnost strojev - Sistem slišnih in vidnih nevarnostnih ali obvestilnih signalov
SIST EN 982:1998	Varnost strojev - Varnostne zahteve za fluidne sisteme in njihove komponente - Hidravlika
SIST EN 983:1998	Varnost strojev - Varnostne zahteve za fluidne sisteme in njihove komponente - Pnevmatika
SIST EN 999:2000	Varnost strojev - Postavitve varovalne opreme glede na hitrosti približanja delov človeškega telesa
SIST EN 1037:1999	Varnost strojev - Preprečevanje nepričakovanega vklopa
SIST EN 1050:2000	Varnost strojev - Načela ocene tveganja
SIST EN 60204-1:1999	Varnost strojev - Električna oprema strojev - 1. del: Splošne zahteve (IEC 60204-1:1997+ corrigendum Sep.1998)

SIST EN 60447:2001	Vmesnik človek-stroj (MMI) – Načela proženja
SIST EN 60529:1997	Stopnja zaščite z ohišjem (IP code) (IEC 529:1989)
SIST EN 60721-3-0:2001	Klasifikacija okoljnih vplivov – 3. del: Klasifikacija skupin okoljnih vplivov in njihova pogostnost – Uvajanje

#### **OSNOVA ZA IZDAJO STANDARDA**

- Prevod standarda EN 954-1:1996.

#### **OPOMBE**

- Povsod, kjer se v besedilu standarda uporablja izraz “evropski standard”, v SIST EN 954-1:2000 to pomeni “slovenski standard”.
- Uvod in nacionalni predgovor nista sestavni del standarda.
- Ta nacionalni dokument je enakovreden EN 954-1:1996 in je objavljen z dovoljenjem

CEN  
Rue de Stassart 36  
1050 Bruselj  
Belgija

This national document is identical with EN 954-1 :1996 and is published with the permission of

CEN  
Rue de Stassart, 36  
1050 Bruxelles  
Belgium

(prazna stran)

ICS: 13.110

Deskriptorji: varnost strojev, krmilne naprave, načrtovanje, vmesniki, nevarnosti, načela, napake, verifikacija

Slovenska izdaja

## Varnost strojev – Deli krmilnih sistemov v zvezi z varnostjo – 1. del: Splošna načela načrtovanja

Safety of machinery – Safety-related parts of control systems – Part 1 : General principles for design

Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze

Ta evropski standard je sprejel CEN dne 1996-07-11. Članice CEN morajo izpolnjevati določila poslovnika CEN/CENELEC, s katerim je predpisano, da mora biti ta standard brez kakršnihkoli sprememb sprejet kot nacionalni standard.

Seznami najnovejših izdaj teh nacionalnih standardov in njihovi bibliografski podatki so na voljo pri osrednjem tajništvu ali članicah CEN.

Evropski standardi obstajajo v treh izvornih izdajah (nemški, angleški in francoski). Izdaje v drugih jezikih, ki jih članice CEN na lastno odgovornost prevedejo in izdajo ter prijavijo pri osrednjem tajništvu CEN, veljajo kot uradne izdaje.

Članice CEN so nacionalne ustanove za standardizacijo Avstrije, Belgije, Danske, Finske, Francije, Grčije, Irske, Islandije, Italije, Luksemburga, Nemčije, Nizozemske, Norveške, Portugalske, Španije, Švedske, Švice in Združenega kraljestva.

### CEN

Evropski komite za standardizacijo  
European Committee for Standardization  
Europäisches Komitee für Normung  
Comité Européen de Normalisation

Osrednje tajništvo: Rue de Stassart 36, B-1050 Bruselj

<b>VSEBINA</b>	<b>Stran</b>
Predgovor .....	3
0 Uvod .....	3
1 Namen .....	4
2 Zveza s standardi .....	4
3 Definicije .....	5
4 Splošna izhodišča .....	5
4.1 Varnostni cilji pri načrtovanju.....	5
4.2 Splošne usmeritve za načrtovanje .....	6
4.3 Postopek izbire in načrtovanje varnostnih ukrepov.....	7
4.4 Načela ergonomskega načrtovanja.....	10
5 Karakteristike varnostnih funkcij.....	10
6 Kategorije .....	16
6.1 Splošno.....	16
6.2 Določanje kategorij.....	16
6.3 Izbira in kombinacija z varnostjo povezanih delov različnih kategorij.....	21
7. Ocenjevanje napak.....	21
7.1 Splošno.....	21
7.2 Izključevanje napak .....	21
8 Vrednotenje .....	22
8.1 Splošno.....	22
8.2 Načrt vrednotenja .....	22
8.3 Vrednotenje z analizo.....	22
8.4 Vrednotenje s preizkušanjem.....	22
8.5 Poročilo o vrednotenju.....	23
9 Vzdrževanje.....	23
10 Navodilo za uporabo .....	24
Dodatek A (informativni): Vprašalnik za postopek načrtovanja.....	25
Dodatek B (informativni): Smernice za izbiro kategorij .....	27
Dodatek C (informativni): Seznam nekaterih pomembnejših napak in odpovedi pri različnih tehnologijah .....	30
Dodatek D (informativni): Povezave med varnostjo, zanesljivostjo in uporabnostjo stroja.....	31
Dodatek E (informativni): Bibliografija .....	32
Dodatek ZA (informativni): Poglavlja v tem evropskem standardu, ki se nanašajo na osnovne zahteve ali druge ukrepe direktiv EU .....	33

## Predgovor

Ta evropski standard je pripravil CEN/TC 114 Varnost strojev, katerega sekretariat vodi DIN.

Ta evropski standard dobi status nacionalnega standarda z objavo istovetnega besedila ali z razglasitvijo, in sicer najpozneje do junija 1996. Nacionalne standarde, ki so v nasprotju s tem standardom, je treba umakniti najpozneje do junija 1997.

Ta standard ima status standarda za uporabo (tip B1) in daje navodila pri načrtovanju in oceni krmilnih sistemov in tehničnim odborom, ki pripravljajo standarde tipa B2 ali tipa C in predvidevajo izpolniti osnovne varnostne zahteve dodatka I direktive Sveta 89/392/EEC in dopolnilnih direktiv 91/368/EEC in 93/44/EEC (glej dodatek A k EN 292-2:1991/A1:1995). Ta standard ne daje posebnih navodil za izpolnitev drugih direktiv EU.

Med predložitvijo tega 1. dela v formalno glasovanje CEN teče priprava 2. dela z naslednjim predvidenim naslovom: "Varnost strojev – Deli krmilnih sistemov v zvezi z varnostjo – 2. del: Vrednotenje" (glej tudi 7. in 8. točko v tem 1. delu.).

OPOMBA: Pri izdelavi 2. dela naj bodo upoštevane zahteve v IEC 1508<sup>1)</sup> "Funkcionalna varnost: Deli krmilnih sistemov, povezani z varnostjo", upoštevajoč potrebe varnosti strojev.

Ta evropski standard je bil pripravljen na osnovi mandata, ki ga je CEN dobil od Komisije Evropske skupnosti in Evropske organizacije za svobodno trgovino in podpira bistvene zahteve direktiv EU.

Za povezavo z direktivami EU glej informativni dodatek ZA, ki je sestavni del tega standarda.

V skladu s poslovnikom CEN/CENELEC morajo uporabo tega standarda uvesti naslednje države: Avstrija, Belgija, Danska, Finska, Francija, Grčija, Irska, Islandija, Italija, Luksemburg, Nemčija, Nizozemska, Norveška, Portugalska, Španija, Švedska, Švica in Združeno kraljestvo.

## Uvod

Deli strojev krmilnih sistemov so pogosto določeni za zagotovitev varnostnih funkcij: imenujemo jih deli, povezani z varnostjo. Ti deli so lahko iz strojne in programske opreme in zagotovljajo varnostno funkcijo v krmilnih sistemih. Lahko so ločeni ali integralni deli krmilnega sistema. Lastnosti z varnostjo povezanega dela krmilnega sistema pri nastanku napak so v tem standardu razdeljene v pet kategorij (B, 1, 2, 3, 4), ki naj se uporabljajo kot referenčne točke. Te kategorije (glej 6.2) niso namenjene za uporabo v kateremkoli danem zaporedju ali hierarhiji v zvezi z varnostnimi zahtevami.

Kategorije se lahko uporabljajo za:

- krmilne sisteme vseh vrst strojev, od enostavnih strojev, npr. malih kuhinjskih strojev, do kompleksnih proizvodnih naprav, npr. embalirnih strojev, tiskarskih strojev, stiskalnic;
- krmilne sisteme varnostne opreme, npr. dvoročna stikala, zaporne naprave, električno občutljive varnostne opreme (npr. fotoelektrične zapore) in preproge, občutljive na tlak.

Izbrana kategorija je odvisna od stroja in obsega, do koder so krmilna sredstva uporabljena za zaščitne ukrepe.

Pri izbiri kategorije in načrtovanju z varnostjo povezanega dela krmilnega sistema je potrebno, da načrtovalec navede vsaj naslednje podatke o delih, povezanih z varnostjo:

- izbrano(e) kategorijo(e),
- funkcionalne značilnosti,
- natančno nalogo, ki jo ima v zaščitnih ukrepih v stroju,
- točne meje (glej 3.1),
- vse upoštevane napake, povezane z varnostjo,

<sup>1)</sup> Standard v pripravi

- z varnostjo povezane napake, ki niso upoštevane pri izključitvi napake, in uporabljeni ukrepi, ki dopuščajo njihovo izključitev,
- parametre, ki se nanašajo na zanesljivost, kot so okoljski vplivi,
- uporabljena(e) tehnologija(e).

Uporaba kategorij kot referenčnih točk in te navedbe za smiseln potek med načrtovalnim procesom omogočajo fleksibilno uporabo tega standarda. Namen je zagotoviti jasno osnovo za ocenjevanje načrtovanja ali lastnosti katerekoli izvedbe. Kjer je primerno, se ta standard lahko uporabi tudi pri delih krmilnega sistema, povezanih z varnostjo, uporabljenih v drugih tehničnih izvedbah, npr. pri tretji strani, interno ali na neodvisnem preskuševališču.

## 1 Namen

Ta evropski standard vsebuje varnostne zahteve in napotke za načela načrtovanja (glej 3.11 v EN 292-1: 1991) delov krmilnih sistemov, povezanih z varnostjo. Za te dele določa kategorije in opisuje lastnosti njihovih varnostnih funkcij. To vključuje programirne sisteme za vse stroje in z njimi povezane varovalne naprave. Uporablja se za vse dele krmilnih sistemov, povezanih z varnostjo, neodvisno od vrste uporabljane energije, npr. električne, hidravlične, pnevmatske, mehanične. Ne določa, katere varnostne funkcije in katere kategorije naj se uporabljajo v posameznih primerih.

Uporablja se za vse izvedbe strojev za profesionalno in neprofesionalno rabo.

## 2 Zveza s standardi

Ta evropski standard vsebuje z datiranim ali nedatiranim sklicevanjem določila iz drugih publikacij. Ta sklicevanja na standarde so navedena na ustreznih mestih v besedilu, publikacije pa so našteve spodaj. Pri datiranih sklicevanjih se pri uporabi tega evropskega standarda upoštevajo poznejša dopolnila ali spremembe katerekoli od teh publikacij samo, če so z dopolnilom ali spremembo vanj vključene. Pri nedatiranih sklicevanjih se uporablja zadnja izdaja publikacije, na katero se sklicuje.

EN 292-1:1991	Varnost strojev - Osnovni pojmi, splošna načela načrtovanja - 1. del: Osnovna terminologija, metodologija
EN 292-2:1991/A1:1995	Varnost strojev - Osnovni pojmi, splošna načela načrtovanja - 2. del: Tehnična načela in specifikacije - Dopolnilo A1
EN 418	Varnost strojev - Oprema za izklop v sili - Funkcionalni vidiki, načela načrtovanja
EN 457	Varnost strojev - Slišni nevarnostni signali - Splošne zahteve, načrtovanje in preskušanje (ISO 7731:1986, modificiran)
EN 614-1	Varnost strojev – Načela ergonomskega načrtovanja – 1. del: Terminologija in splošna načela
EN 842	Varnost strojev - Vidni nevarnostni signali - Splošne zahteve, načrtovanje in preskušanje
EN 981	Varnost strojev - Sistem slišnih in vidnih nevarnostni ali obvestilnih signalov
EN 982	Varnost strojev - Varnostne zahteve za fluidne sisteme in njihove komponente - Hidravlika
EN 983	Varnost strojev - Varnostne zahteve za fluidne sisteme in njihove komponente - Pnevmatika
prEN 999 :1995	Varnost strojev - Postavitev varovalne opreme glede na hitrosti približanja delov človeškega telesa



EN 1037	Varnost strojev - Preprečevanje nepričakovanega vklopa
EN 1050:1996	Varnost strojev - Načela ocene tveganja
EN 60204-1:1992	Varnost strojev - Električna oprema strojev - 1. del: Splošne zahteve
EN 60447:1993	Vmesnik človek-stroj (MMI) – Načela proženja
EN 60529	Stopnja zaščite z ohišjem (IP code) (IEC 529:1989)
EN 60721-3-0	Klasifikacija okoljnih vplivov – 3. del: Klasifikacija skupin okoljnih vplivov in njihova pogostnost – Uvajanje
IEC 50 (191):1990	Mednarodni elektrotehniški slovar, poglavje 191: Zagotovitljivost in kakovost oskrbe

### 3 Definicije

Pri uporabi tega standarda veljajo definicije iz EN 292 – 1 in IEC 50 (191), skupaj z naslednjimi:

**3. Deli krmilnega sistema, povezani z varnostjo:** Del ali podrejeni del(i) krmilnega sistema, ki se odziva(jo) vhodnim signalom in proizvaja(jo) z varnostjo povezane izhodne signale. Kombinirani deli krmilnega sistema, povezani z varnostjo, se začenejo tam, kjer nastajajo z varnostjo povezani signali, in končajo pri izhodu elementov za krmiljenje energije (glej tudi dodatek A k EN 292-1: 1991). To vključuje tudi nadzorne sisteme.

**3.2 Kategorija:** Razvrstitev delov krmilnega sistema, povezanih z varnostjo, glede na njihovo odpornost proti napakam in njihovo kasnejše obnašanje pri napaki in glede na to, kar je doseženo s strukturno namestitvijo delov in/ali njihovo zanesljivostjo.

**3.3 Varnost krmilnih sistemov:** Sposobnost delov krmilnega sistema, povezanih z varnostjo, za izvajanje varnostnih funkcij za določeno časovno obdobje v zanje določeni kategoriji.

**3.4 Napaka:** Stanje predmeta, opredeljeno z nezmožnostjo opravljati zahtevano funkcijo, izključujoč to nezmožnost med preventivnim vzdrževanjem ali drugimi hotenimi posegi ali zaradi manjkajočih zunanjih virov.

OPOMBA 1: Napaka je pogosto posledica odpovedi samega predmeta, lahko pa nastane brez predhodne odpovedi.

OPOMBA 2: V angleščini sta izraz "fault" in njegova definicija identična s tistima v IEC 50 (191) : 1990. Na področju strojev se francoski izraz "défaut" in nemški izraz "Fehler" bolj uporabljata kot izraza "panne" in "Fehlzustand", ki se pojavljata v tej definiciji.

**3.5 Odpoved:** Prenehanje sposobnosti nekega predmeta, da opravlja zahtevano funkcijo.

OPOMBA 1: Po odpovedi ima predmet napako.

OPOMBA 2: Odpoved je posledica, v nasprotju z napako, ki je stanje.

OPOMBA 3: Tako definiran pojem ne velja za predmete, ki so le v programski opremi (IEV 191-04-01 v IEC 50(191): 1990).

OPOMBA 4: V praksi se izraza napaka in odpoved pogosto uporabljata kot sinonima.

**3.6 Varnostne funkcije krmilnih sistemov:** Funkcija, sprožena z vhodnim signalom in procesirana (predelana) v delu krmilnega sistema, povezanem z varnostjo, ki omogoči stroju (kot sistemu) doseči varno stanje.

**3.7 Muting:** Začasna avtomatična prekinitve varnostne(nih) funkcije(j) s pomočjo delov krmilnega sistema, povezanih z varnostjo.

**3.8 Ročna ponovna vzpostavitev:** Funkcija v delih krmilnega sistema, povezanih z varnostjo, za ročno obnovitev dane varnostne funkcije pred ponovnim vklopom stroja.

## 4 Splošna izhodišča

Deli krmilnega sistema, povezani z varnostjo, ki opravljajo varnostne funkcije, morajo biti načrtovani in konstruirani tako, da so v celoti upoštevana načela iz EN 1050:

- pri vseh namembnih uporabah in predvidljivi zlorabi,
- pri nastanku napak,
- pri predvidljivih človeških napakah med namembno uporabo stroja kot celote.

### 4.2 Splošna strategija načrtovanja

Z vidika ocene tveganja (glej EN 1050) na stroju mora načrtovalec odločati o zmanjšanju tveganja, ki naj ga prispeva vsak del krmilnega sistema, povezan z varnostjo (glej dodatek B). Ta prispevek ne pokriva celotnega tveganja krmiljenega stroja, npr. ni upoštevano celotno tveganje mehanske stiskalnice ali pralnega stroja, ampak tisti del tveganja, ki je zmanjšano z uporabo določene varnostne funkcije. Primeri takih funkcij so ustavitvena funkcija, dosežena z uporabo električno občutljive zaščitne naprave na stiskalnici, ali funkcija zaklepanja vrat v pralnem stroju.

Ključni cilj je, da mora načrtovalec zagotoviti, da deli krmilne naprave, povezani z varnostjo, dosežejo učinke, ki zmanjšajo tveganje po EN 1050. To ni vedno dosegljivo in v takih primerih mora načrtovalec določiti druge varnostne ukrepe. Hierarhija strategije zmanjševanja tveganja je dana v 5. točki v EN 292 – 1: 1991.

Kategorija in druge poteze, npr. fizična namestitvev delov, izolacija, ki jo izbere načrtovalec za dele, povezane z varnostjo, so odvisni od prispevka teh delov k zmanjšanju tveganja, od načrtovanja in tehnologije (glej točko 0). Načrtovalec mora podati:

- katera(e) kategorija(e) je bila uporabljena pri načrtovanju kot referenčna točka;
- točne točke, kjer se deli, povezani z varnostjo, začnejo in kje končajo;
- smiselno načrtovanje, npr. upošteevane napake, izključene napake pri načrtovanju za dosego teh kategorij.

Čim bolj je zmanjšanje tveganja odvisno od delov krmilnega sistema, povezanih z varnostjo, toliko bolj se zahteva večja odpornost teh delov proti napakam. Ta sposobnost – s pogojem, da je zahtevana funkcija izvedena – je lahko delno izmerjena z vrednostjo zanesljivosti in s strukturo odpornosti proti napakam. Obe, zanesljivost in struktura, prispevata k odpornosti proti napakam delov, povezanih z varnostjo. Navedena odpornost proti napakam se lahko doseže z določeno stopnjo zanesljivosti komponent in/ali z izboljšano strukturo z varnostjo povezanih delov. Prispevek zanesljivosti in strukture se lahko spreminja z uporabljeno tehnologijo. Tako je npr. možno za enojen kanal z varnostjo povezanih delov visoke zanesljivosti v neki tehnologiji doseči enako ali večjo odpornost proti napakam kot pri strukturi manjše zanesljivosti, tolerantni za napake, v neki drugačni tehnologiji.

OPOMBA: Čim višja je odpornost do napak z varnostjo povezanih delov, toliko nižja je verjetnost, da odpovedo z varnostjo povezani deli pri izvajanju zahtevanih varnostnih funkcij.

Zanesljivost in varnost ni isto (glej dodatek D). Npr. možno je, da je varnost sistema z relativno nezanesljivimi komponentami v strukturi preobilja večja kot varnost sistema z enostavnejšo strukturo, vendar z bolj odpornimi komponentami. Ta koncept je pomemben, ker v nekaterih aplikacijah varnost zahteva višjo prioriteto ne glede na doseženo zanesljivost, npr. če so posledice napake vedno resne in običajno nepopravljive. V takih aplikacijah se mora skladno z oceno tveganja predvideti zaznavanje napak (toleranca napake v enem ciklu) strukture, ki omogoči zahtevano varnostno funkcijo po eni, dveh ali več napakah.

Ta standard ne zahteva izračuna vrednosti zanesljivosti za kompleksne strukture, kjer je varnost dosežena pretežno z izboljšanjem strukture z varnostjo povezanih delov. Pri manj kompleksnih strukturah, kjer je zanesljivost komponent pomembna za varnost, je izračun vrednosti zanesljivosti koristen pokazatelj prispevka delov, povezanih z varnostjo, k celotnemu zmanjšanju tveganja.

V primeru aplikacij z majhnim tveganjem so ukrepi za preprečitev napak lahko primerni; pri aplikacijah z večjim tveganjem se lahko z izboljšavo strukture delov krmilnega sistema, povezanih z varnostjo,

dosežejo ukrepi za preprečitev, zaznavo ali toleriranje napak. Praktični ukrepi vključujejo preobliko presežek, različnost, nadzorovanje (glej tudi 3. točko v EN 292-2:1991, dodatek A v EN 292-2:1991/A1:1995 in 9.4 v EN 60204-1:1992).

Doseženo obnašanje glede na odpornost proti napakam delov krmilnega sistema, povezanih z varnostjo, je funkcija več parametrov, npr.:

- zanesljivost z vidika izvajanja varnostnih funkcij,
- struktura (ali arhitektura) krmilnega sistema,
- kvaliteta z varnostjo povezane dokumentacije,
- popolnost specifikacije,
- načrtovanje, izdelava in vzdrževanje,
- kakovost in pravilnost programske opreme,
- obseg preskusov funkcionalnosti,
- obratovalne lastnosti krmiljenega stroja ali krmiljenega dela stroja.

Ti parametri se lahko razvrstijo na osnovi treh glavnih značilnosti:

- zanesljivost strojne opreme – stopnja zanesljivosti komponent za preprečevanje napak;
- struktura sistema – namestitev komponent v delih krmilnega sistema, povezanih z varnostjo, za preprečitev, toleriranje ali zaznavanje napak;
- kakovostni vidiki, ki se ne dajo ovrednotiti, ki vplivajo na obnašanje delov krmilnega sistema, povezanih z varnostjo.

#### 4.3 Postopek za izbiro in načrtovanje varnostnih ukrepov

To podpoglavje podaja postopek za izbiranje razpoložljivih varnostnih ukrepov in za načrtovanje delov krmilnega sistema, povezanih z varnostjo. Pomembno je določiti povezavo med deli krmilnega sistema, povezanimi z varnostjo, deli, ki niso povezani z varnostjo krmilnega sistema, in vsemi drugimi deli stroja. Nato se lahko določi zmanjšanje tveganja, ki ga prispevajo deli krmilnega sistema, povezani z varnostjo, v okviru ocene tveganja stroja skladno z EN 1050.

Ker je več možnosti za zmanjšanje tveganja na stroju in več možnosti, kako se lahko načrtujejo deli krmilnega sistema, povezani z varnostjo, je ta proces iterativen. Na odločitve in/ali predvidevanja, sprejete pri vsakem koraku v procesu, lahko vplivajo odločitve in/ali predvidevanja, sprejete pri predhodnem koraku. Ta vidik se lahko preveri s ponovitvijo procesa na vsakem koraku. To preverjanje po korakih je bistvenega pomena, da se doseže varnostna zahteva, ki je enaka tisti v specifikaciji.

Postopek je prikazan v sliki 1. Pomembni vidiki, ki naj bodo upoštevani pri procesu načrtovanja, so navedeni kot vprašanja za miselno vzpodbudo načrtovalcu v dodatku A. Ta vprašanja podajajo filozofijo, ki naj ji sledi načrtovanje z varnostjo povezanih delov. Vsa vprašanja ne veljajo za vsako aplikacijo; nekatere aplikacije zahtevajo dodatna vprašanja.

1. korak: Analiza nevarnosti in ocena tveganja

- Določitev prisotne nevarnosti na stroju med vsemi načini delovanja in na vsaki stopnji življenjske dobe stroja, skladno z navodili v EN 292-1 in EN 1050.
- Ocenitev tveganj, ki nastanejo zaradi take nevarnosti in določitev primerne zmanjšanja tveganja za to uporabo, skladno z EN 292-1 in EN 1050.

2. korak: Odločanje o ukrepih za zmanjšanje tveganja s krmilnimi sredstvi

- Odločanje o načrtovanih ukrepih na stroju in/ali predvideni zaščiti za dosego zmanjšanja tveganja. Ti deli krmilnega sistema, ki sodelujejo kot sestavni del načrtovanih ukrepov in/ali pri krmiljenju zaščitne opreme, se morajo šteti za dele, povezane z varnostjo.